CSC2125 Homework 5

Zi Han Zhao

1001103708

1 What would happen if a powerful attacker identifies all participants of one shard in OmniLedger and launches DDoS attacks to take down the participants of the shard (make them offline)? Will this attack affect transactions in other shards?

2 What would happen if the attacker is able to even bribe the participants to process invalid transactions? Will this attack affect transactions in other shards?

3 Is Monoxide running 64 parallel Nakamoto consensus chains (without Chukonu mining) less secure than the original Bitcoin consensus? Why?

4 Suppose a Monoxide node is using Chukonu mining on k shards. How many resources (e.g., storage, computation, etc.) the node would need comparing to a node without Chukonu mining? Is sharding really useful in this Chukonu mining case?